A COST EFFECTIVE, INTEGRATED AND SMART RADIOACTIVE SAFEGUARD SYSTEM

A Thesis

by

HARNEET SINGH

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

December 2010

Major Subject: Electrical Engineering

A COST EFFECTIVE, INTEGRATED AND SMART RADIOACTIVE SAFEGUARD SYSTEM

A Thesis

by

HARNEET SINGH

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Approved by:

Chair of Committee,	Jim X. Ji
Committee Members,	Mehrdad Ehsani
	Raffaella Righetti
	M. Suhail Zubairy
Head of Department,	Costas N. Georghiades

December 2010

Major Subject: Electrical Engineering

ABSTRACT

A Cost Effective, Integrated and Smart Radioactive Safeguard System. (December 2010)

Harneet Singh, B.S., Texas A&M University

Chair of Advisory Committee: Dr. Jim X. Ji

Nuclear energy is a growing field worldwide due to its wide range of applications in various walks of life. It, however, deals with radioactive materials, specifically special nuclear material, which, if misused, could result in catastrophic consequences. In order to protect this precious resource and ensure its use for the good of mankind, safeguard systems are more important than ever. Current Market solutions are wide ranged but have a large number of disadvantages, some of which include high cost, constant updates, and incomplete efforts. The rising need of a cost effective, efficient, and integrated radioactive safeguard system serves as motivation for the solution outlined in this thesis. The thesis outlines a solution structured around the three pillars of the international safeguards program, namely, visual surveillance and motion detection, containment analysis, and non-destructive analysis. The hardware around each of these pillars work together with a clean and user-friendly application to provide a secure safeguards system that is both flexible and extensible.

To my family for their love, support, and encouragement.

ACKNOWLEDGEMENTS

I would like to thank my advisor, Dr. Ji, for his guidance, support, and assistance throughout the course of my study. I would also like to thank my committee members, Dr. Ehsani, Dr. Righetti, and Dr. Zubairy, for their guidance and support throughout the course of this research.

I also want to extend my gratitude to Mr. Claudio Gariazzo of Texas A&M University for his assistance, as well as the Department of Nuclear Engineering and National Security Sciences and Policy Institute for providing me with the data that I used in my research. Thanks also go to my friends and colleagues and the departmental faculty and staff for making my time at Texas A&M University a great experience.

Finally, thanks to my family for their encouragement and continuous support.

NOMENCLATURE

ADC	Automatic Data Collection
AVI	Audio Video Interleave
BAP	Battery Assisted Passive
BMP	Bitmap
CCTV	Closed-Circuit Television
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical Equipment
JPEG	Joint Photographic Experts Group
LED	Light Emitting Diode
MC&A	Material Cost & Acoounting
MDI	Multiple Document Interface
MJPEG	Motion JPEG
MMS	Microsoft Media Services
MPEG	Motion Pictures Expert Group
NDA	Non-Destructive Analysis
NSSPI	Nuclear Security Sciences and Policy Institute
PLC	Programmable Logic Containers
PTZ	Point to Zoom
RFID	Radio Frequency Identifier

SNM	Special Nuclear Materials
UHF	Ultra High Frequency
UI	User Interface
USB	Universal Serial Bus

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF CHARTS

LIST OF TABLES

TABLE Page

1. INTRODUCTION

1.1 Problem Statement and Overview

The resurgence of nuclear energy is leading to a number of nations having (or wanting) nuclear material for powering nuclear reactors. Although it is acceptable to use these to produce the needed electricity, nuclear reactors have been used for other non-peaceful uses as well. The intent of international inspections is to assure global community of the state's benevolent intention and to foster trust. A state must adopt a state system of accounting and control that is verified by international bodies. These verifications form the basis of an effective safeguards system for the nation. The special nuclear material (SNM) i.e. reactor fuel must be accounted for at all times and is done by employing material accounting, control and physical system.

The material control and accounting system comprises of various components that account for the SNM via surveillance, containment, and radiation detection and quantification (Non Destructive Analysis (NDA)). Other components exist but these three are essential to the developed system here. These three facets create the pillar of the material control and accounting (MC&A) system developed and deployed in this project: visual surveillance, containment analysis via electronic item tracking, and radiation sensing.

The journal model is *IEEE Transactions on Automatic Control*.

To date, market solutions have proven to be expensive, incomplete, and in need of constant updates. Solutions that exist and continue to be produced in the market are targeted mainly for homeland security. However, with the growing need and use, a cost-effective, integrated, and robust solution is desired. With regulations and guidance being continually updated, the system needs to be flexible and extensible as well as simple to update and maintain.

The three pillars of the international safeguards program - visual surveillance and motion detection, containment analysis, and non-destructive analysis (NDA) – are used to model the solution outlined in the thesis. Visual surveillance and motion detection is achieved through the use of cameras – Internet Protocol (IP) based and Point to Zoom (PTZ). Containment analysis is achieved through the use of Radio Frequency Identifier (RFID) tags and readers. NDA is achieved through the use of radiation detectors. When combined together, these three pillars offer an end-to-end secure solution.

However, the hardware alone does not offer a complete solution. In order to ensure that the hardware works together in an efficient and user-friendly manner that can be used widely, the thesis also outlines applications for each of the above. The three applications developed for the individual purposes are combined together in a simple tabbed application that allows monitoring using visual surveillance and motion detection, RFID monitoring, and radiation detection.

When compared to market solutions present today, this solution is cost-effective, efficient, complete, easy to maintain, flexible, extensible, and robust. The next section gives an outline of the thesis.

1.2 Outline of Thesis

The thesis begins with some background on the importance of solving this problem and the need for a secure solution. This includes a deep dive into the problem space as well as an overview of existing market solutions. The background sections also outlines the challenges faced during the development of this thesis project. This followed by the main section on the integrated safety solution. This consists of a detailed description of the hardware used, the algorithms and testing used in software development, and concludes with the results and analysis of the research.

2. BACKGROUND

2.1 Nuclear Security and Safeguards

Most of us know that nuclear science has become an integral part of our world. Nuclear science has its applications today in a wide variety of areas ranging from daily energy production to the field of medicine. However, radioactive materials can be misused if acquired by dangerous hands, including terrorist organizations. As a result, the threat of nuclear terrorism is of great concern today especially following the events of the last few years.

The topic of nuclear security today is considerably more intricate than it was during the Cold War. And, there has always been a constant need to safeguard and protect radioactive materials, specifically SNM that comprises both fresh and spent nuclear fuel, which contain uranium and plutonium. A society with a high degree of "nuclear security" would be one very different from the one we live in today. It would be one with greatly reduced risks and a world confident in expanding its realization of the benefit of civil nuclear power [1].

Threats become far less probable if the authorities possessing SNM have knowledge of the quantity , its location, and can ensure security from theft or loss on a real time basis. Further, to foster global confidence, it behooves the state to have international verification of its system of accounting and control and assure others that the state has control over all SNM. The scientific technology and development required for such an ideal scenario is broad. It covers a range of disciplines such as nuclear

physics, engineering, chemistry, material sciences, image processing, large-scale computation, modeling, and radiation detector development among many others. Considering threats continue to evolve and present themselves,, security policies and methodologies must sustain a level of proficiency in providing sufficient confidence that SNM is safely guarded.. As a result of these ever changing threats and guidelines, the requirements and baseline for the technology keep getting updated for hardware, software, and their development.

Since safeguarding nuclear material involves intensive collaboration between engineering, technology, and policy, the field is challenging. This makes the ideal scenario described above difficult to achieve. Even a small change in the hardware involved in a security system (for example a video camera) requires a major update in the software controlling it and vice versa. To illustrate - if one were to purchase a new camera supporting 10X digital zoom and the old software supported only a 5X zoom, using the new camera would require the software to be updated not only to support a 10X zoom but also to provide better image encoding and decoding techniques using the least amount of resources. Similar problems are faced when there are updates to radiation detectors or any other equipment used in a material safety system.

Current government regulations require that policies concerning safeguard and security of radioactive materials be updated every year [2]. Due to this and the fact that new discoveries are still being made in the field, update costs for the security equipment every other year can run into tens of thousands of dollars. These costs increase sharply when one takes into consideration the number of man-hours lost in bringing security

personnel up to date with the new technology employed. Also, one needs to realize the fact that the newly purchased technology cannot be implemented immediately as they must first be validated and certified for use in secure facilities. In general, while dealing with radioactive material, such a breach of security can lead to serious implications for the individual and society as whole. These are a few problems plaguing the field of nuclear security. Some others include implications in the field of social sciences such as public policy, international relations, and economics.

2.2 Current Market Solutions

From the discussion above, it is quite clear that nuclear security is multidisciplinary due to its technological and social aspects. Various commercial enterprises offer technological solutions available in the market today. Well-known companies such as Canberra, Princeton Gamma-Tech, Gamma Products, and Alpha Spectra etc. have developed solutions that aid in safeguarding nuclear materials. Since these companies are over 40 years, they have the best technological know-how to manufacture such systems. At the same time, a strong financial base helps them update their product as per new regulations every year. However, secure facilities are never "clean-cut" to use one system for one type of material out right. Worldwide, these facilities have been in existence for so long that their safeguards and security system are a random collection of technologies collected over the decades. Many times they are retrofitted with already outdated hardware and software.

A major disadvantage of these solutions is an update to the system. The hardware and software updates, every two years can cost anywhere up to $1 million and are not feasible, especially if a combination of systems is employed (which is usually the case). Another disadvantage is that these systems offer only Non-destructive analysis (radiation measurements) as the primary, albeit incomplete solution. For material accounting, these types of systems can be adequate if their measurements give assurance that no material has been diverted. This would be cost prohibitive and intrusive to the facility. To mitigate this, material control is the concept that after the material is accounted for; systems must exist to ensure that the measured data is accurate and precise between measurements. These systems (comprised of cameras, motion sensors, and seals) thus provide for a continuity of knowledge. Another reason for wanting to develop an independent system is the lack of customization in current market offerings. Current solutions available in the market tend to prioritize flexibility low on their list. Many users look for flexibility while making purchases to suit their varied applications. Most solutions are developed either for homeland security purposes or for scanning large transportation vehicles such as trains and trailers or for large sites comprised of various facilities (whereas Texas A&M University's facility is a small, static facility). As a result, they are extremely huge, power hungry, inefficient, and not adaptable to specific indoor applications such as lab experimentation, simulation analysis or for teaching courses.

2.3 System Development

As discussed in the previous sections, the current market solutions are either

- Incomplete
- Too expensive to maintain and update
- Require training before they can be utilized to their maximum potential
- Too large for the task at hand

The goal of this project implemented through the Nuclear Security Sciences & Policy Institute (NSSPI), housed in the Department of Nuclear Engineering at Texas A&M University is to develop a low cost material control and accounting system (that would feed into a larger safeguards system) that achieves all of the above and much more. Such a system consists of different components feeding information into an integrated user-friendly software interface for easy viewing and operation. The system consists of hardware that is vendor independent, is assembled using off the shelf components, and has on-par or better capabilities than existing market solutions. This is designed as an intelligent plug and play system that can be used with any equipment independent of hardware manufacturer. It uses intelligent software and algorithms that integrate different hardware layers together, thus providing all the necessary information in a simple and user-friendly fashion to the end-user.

While providing an efficient, end-to-end solution, such an integrated system demonstrates the concepts of applied safeguards technology and allows students to practice nuclear security techniques with tools that are currently used in the field as an added benefit. In general, it accomplishes these basic goals for coursework:

- Provide necessary classroom fundamentals in nuclear security sciences
- Understand the unique challenges that arise when applying classroom concepts to real-world problems
- Provide an opportunity for hands-on training (lab experiments, simulations etc.)[1]

The system can also be used for graduate level research and development projects in a significant manner. It demonstrates and practices three essential components of an integrated material control system which potentially feeds into an international safeguards program:

- Visual Surveillance and Motion Detection
- Containment Analysis
- Radiation Detection [1]

Visual surveillance is the oldest and most direct form of surveillance for any security system. It is done using cameras that inspect and observe an area. The cameras are connected over an IP network and the transmission is watched over by security personnel. However, it has been noted that any security system cannot be watched over 24 hours a day and usually requires some form of automated surveillance. As such, highly efficient motion detection software exclusive to our system is developed. This motion detection algorithm is protected by a code that is changed daily for further security. Containment analysis combined with visual surveillances form the second pillar of our safeguards technology. Along with tamper indicating devices, we utilize Radio Frequency Identification (RFID) and its middleware as an extra layer of containment

surveillance. NDA equipment and software tools provide for gamma detection, spectroscopy, and neutron counting. This specifically involves using radiation detectors, also known as gamma ray detectors. They are used to detect, track, and/or identify high-energy particles (gamma rays) produced by radiation.

To summarize, the main goal of the proposed solution is to make all three pillars come together under a single roof through an application that provides flexibility and extensibility to the user. The application is designed to be plug and play for ease of use. This simply means that the application is capable of detecting any hardware that is connected to the system on its own. It then adapts itself to show relevant information to the user. It is developed using open source languages and libraries available through C# and Java. Moreover, Microsoft Visual Studio is actively employed as a development tool to periodically automate and test the software, as software is developed to ensure reliability and content management.

2.4 Challenges

Due to the technical nature of this project, ever changing regulations in the field of nuclear security, continuous software development, and constraints offered by the hardware, there will be few challenges that were faced during development. These are:

- Integration: As the thesis title suggests, one of the main goals is to create an integrated system, which combines together all the three pillars of international nuclear safeguards. However, incorporating different pieces of equipment such as cameras, Geiger counters, RFIDs from different

manufactures into single system is one the main challenges. At the same time, we also have to integrate the input from the equipment in such a way that a real time status update is provided to the user at all times. To define more closely, the challenge of integration can be further divided into the following categories:

- *Integration of various image formats:* BMP, MJPEG, AVI etc. are just a few of the image and video formats widely used today across all operating platforms. Our software system brings together all the formats in the market for processing. A risk of supporting multiple formats was the probability of the software being resources hungry and thus slowing down overall system performance. This risk was mitigated by paying particular attention to the efficiency of the algorithm throughout the course of development.
- *Software Limitations:* Currently, no software in the market is capable of integrating equipment from different manufacturers and displaying information on a single screen. This is due to the fact that all manufacturers aim to promote their product. Due to this, they follow a closed model. This is despite the fact that all available hardware uses the same transmission and communication protocols (USB, RJ-45, RS232 etc.). Due to

various copyright and legal issues, our software is developed using open source resources available in C# and Java.

- Cost Effectiveness: We are fully aware of the current market solutions offered by different manufacturers. We also know that these solutions are not only expensive but also incomplete since they require additional components that increase the system cost manifold. Apart from this, any updates to the system require security personnel to be trained to effectively use the updated system. These factors combined with few listed below increase the current market system costs a lot.
    - Storage Constraints: The storage limitations of the equipment being used. These limitations and challenges arise due to the presence and use of cameras and RFID. The need to store historical events or archive information from camera feed and RFIDs is absolute and also gives rise to this particular challenge.
        - The current storage per megapixel in the cameras is too expensive. Storing every frame recorded by the camera poses a big system burden and could result in a storage system spanning several terabytes. Although various storage systems are available in the market that can match our needs, adding them will just increase the complexity and cost of any system. If the user were to search for a specific event, it would require going through all the recordings unless a video search

algorithm is used. Unfortunately, current video search algorithms are either highly complex, or ineffective, or very costly. The solution is thus to develop an in-house motion detection algorithm that would record only the events based on information provided by the user. This would not only reduce the storage and development costs but also provide smartness to the system.

- A similar storage challenge was faced with RFID systems. Supply chain traceability and real time tracking drive the need to store operational data. However, current databases that are used to store traditional transactional data are not capable of handling such a load. The mitigation used for this is hash tables.

- *Missed and Unreliable RFID Readings:* This challenge is very common among cheaper RFID equipments available in the market. As mentioned, it usually happens when using cheap and low power hardware for wireless communications. Factors such as reflection of radio waves from metallic objects nearby also give rise to this problem. Although use of expensive RFID antennas and tags can overcome the problem, it will add to the system cost and defeat the purpose. Installing RFID in an environment that allows obstacle free transmission of radio waves upon which they

operate can mitigate this problem. However, relying on physical environment is not enough since environment and surroundings are subject to change. A combination of correct RFID installation and hash tables' solutions will be used in the software to effectively overcome this hurdle.

- Smartness: A universal hardware accepting security system i.e. a plug and play system is what we aim to achieve with this research. Along with this capability, we also aim to develop smart individual software driving various hardware components used. This software smartness is necessary to achieve performance optimization as well as provide the user with the best available data about the surroundings. The list of smart software solution applied to the equipment is as follows:
    - *Geiger Counters:* Geiger Counters or radiation monitors can sweep only limited area for detecting radiation. An increase in sweep area can be achieved only by steeply increasing the cost of the counter. The aim of our system is to be cheaper, smarter and more effective when compared to available commercial systems. To achieve this, using 'Monte-Carlo' algorithm for radiation detection mitigates the problem posed by Geiger Counters.
    - *Cameras:* As mentioned before, cameras will be utilizing a smart motion detection algorithm to record and report events that match the description and sensitivity level provided by the user

beforehand. If the user provided criteria is met, the software is also capable of taking actions such as launching an application or sounding an alarm to alert the user about the activity.

Being the main objectives of this research, the solutions outlined next address the challenges listed above.

3. INTEGRATED SECURITY SYSTEM

3.1 Equipment

Our security system is based on three main pillars for an integrated international safeguards program, namely:

- Visual Surveillance and Motion Detection
- Containment Analysis
- Radiation Detection
- Material Tracking

This means that equipment covering each of the three pillars forms the very foundation of this integrated security system. While visual surveillance is done with the aid of cameras and a motion detection algorithm, containment analysis requires the use of RFIDs. Last but far from the least, NDA is achieved using radiation monitors. Integrating these three pillars under a common roof using the means of software is what brings uniqueness to the system.

3.1.1 Cameras

Visual surveillance is an integral part of any security system and acts as the first stage of deterrent in a MC&A system. Any modern day security system uses surveillance cameras to visually inspect and observe an area. These cameras are often connected to a recording device, IP network, or watched over by security personnel. For our purpose, we look at two main categories of cameras available in the market:

- Fixed IP Cameras
- Pan-Tilt-Zoom (PTZ) IP Cameras

3.1.1.1 Fixed IP Cameras

IP cameras are closed circuit television cameras that use an Internet protocol to transmit data and control signals over a fast Ethernet link.

A fixed IP camera is the best choice when a traditional camera design is preferred for deterrence. The viewing direction is set once the camera is mounted. There are several models with vari-focal lens and/or exchangeable lenses for increased flexibility.

Fixed cameras are mounted in a stationary position (although what the camera is mounted on may move, such as when used on a police vehicle). These cameras view the same scene until physically relocated. The scene is typically recorded and, less often, security personnel also view the scene simultaneously on a monitor.

A few advantages offered by fixed IP cameras are:

- Cheaper to use
- 2 way audio allow users to communicate what they are seeing
- LED lighting used for night vision
- Ability to view at a streaming rate
- Modern day fixed IP cameras can be installed and used on the wireless network

Despite its many advantages, fixed IP cameras are stationary and so cannot rotate or change their viewing angle remotely or by themselves. As such they have to be used in combination with cameras which can be rotated, panned and are controlled remotely i.e. PTZ cameras.

3.1.1.2 PTZ Cameras

A PTZ camera is a closed circuit television camera with remote directional and zoom control. PTZ is used in two contexts within the video security and surveillance products industry. First, PTZ is an acronym for pan, tilt, and zoom and may refer merely to features of specific surveillance cameras. Second, PTZ cameras may also be used to describe an entire category of cameras where a combination of sound and/or motion and/or change in heat signature may enable the camera to activate, focus and track suspected changes in the video field. By activating only during times of change, systems can notify human monitors and minimize storage requirements.

Some advantages offered by PTZ cameras are:

- Monitoring large areas: the PTZ camera can be pan, tilted and zoomed to cover hundreds of acres (a few square kilometers). This is not possible with fixed cameras which normally only cover a small area (few hundred square meters).
- PTZ cameras can be placed on tours (patterns) that move the camera in a predetermined way to capture areas of interest. For instance, over a 1-minute period, the camera can capture the front door, the gate to the parking lot and

the fence line. The tour can repeat indefinitely.

- Because PTZ cameras can cover a wide area, this reduces the cost of coverage per given area.

Some disadvantages of PTZ cameras are as follows:

- PTZ cameras can see and record only where they are currently looking. While they have the potential to view enormous areas, at any given time, it only covers the area of a fixed camera. If a PTZ camera on a tour is looking at the front door and an event happens at the vehicle gate, that event is missed (and vice versa). Using cameras at all the points of interest however, can solve this.
- Incorrect positioning of PTZ cameras is common. Operators routinely place (or leave) the PTZ in different positions. While using a 'home' functionality (set to default position) can solve this, many systems are not configured to use this properly.
- Works Poorly over IP Networks: Controlled mechanically, PTZ cameras are very sensitive to latency. If the latency is more than a fraction of a second, controlling PTZ cameras become very difficult. This is not an issue for traditional analog systems but a growing problem for IP video. Furthermore, network viewing often requires on screen PTZ controls which are much harder for an operator to use. These issues can be somewhat rectified by using USB joysticks and software optimizations to reduce latency.

To overcome a maximum number of shortcomings of CCTV cameras, the

solution is to deploy a combination of fixed IP and PTZ cameras.

For fixed IP cameras, the Axis 211A shown in Figure 1 has been employed. It has the following advantages:

- Superior image quality with progressive scan
- A high resolution of 640*480 pixels (highest available in its class)
- Professional video with two-way built in audio over Ethernet networks
- Vari-focal lens allowing for illumination in low light conditions and quick adjustment for outdoor lightning

Figure 1: Axis 211A IP Network Cameras

Similarly, an Axis camera model Axis 213 PTZ shown in Figure 2 is used as the Pan-Tilt-Zoom Camera. It has the following advantages:

- Pan, tilt, zoom network camera with built-in 26x optical zoom, auto focus lens with 12x digital zoom
- Operates under all light conditions, both indoors as well as outdoors
- Connection Module for two-way audio and alarm inputs/outputs
- Built in video-motion detection

Figure 2: Axis 213 PTZ Cameras

3.1.2 Radio Frequency Identification (RFID)

Using RFID carries out the second pillar of our security system - containment analysis. They also supplement the NDA monitors to monitor material movement. This is one of the fastest growing and most beneficial technologies being adopted by various businesses and laboratories today. Scientists consider RFID technology as nothing less than an embodiment of the paradigm shift towards ubiquitous computing. Companies are increasingly viewing it as an advanced means towards cost savings, efficiency gains, and unprecedented product tracking [3]. RFID automatic data collection (ADC) technology is also being increasingly adopted due to the establishment of key standards, government mandates, improved technology, and falling implementation costs [4].

The word "RFID" is associated with technology that aids in receiving and sending data wirelessly. It, therefore, consists of wireless exchange of information between a tagged object and a reader/writer. As such, an RFID system contains the following components:

- Tags (or transponders), which consist of a semiconductor chip and antenna
- Read/write devices called readers (or interrogators)
- Antennas, separately on the tag and each reader
- Application software running on a computer system

The tags store unique information about an item in its chip. These tags are then applied to the items that need to be read. They can be placed either directly on the item using an adhesive or hidden in an enclosure. Readers are placed at the point of interest, a door, hallway, or any other area that needs to be monitored for activity. The reader

transmits a radio signal at a preset frequency to the tags. The tags respond by transmitting stored data. The reader, after receiving the data signal via its antenna, decodes the data and transfers it to the application running on the computer system. Figures 3 and 4 illustrate the RFID tag and working of RFID system respectively [4].

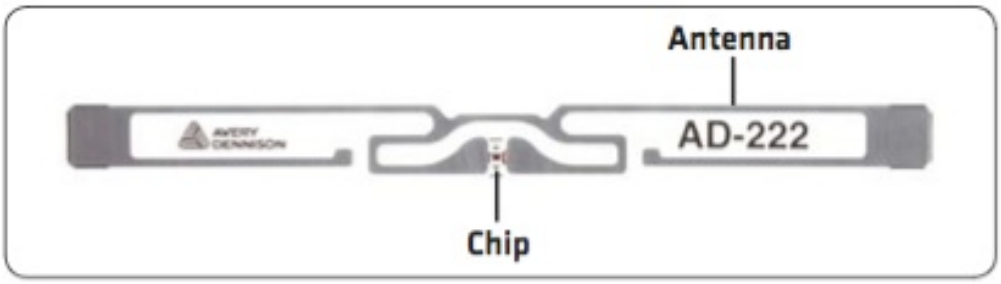

Figure 3: RFID Tag

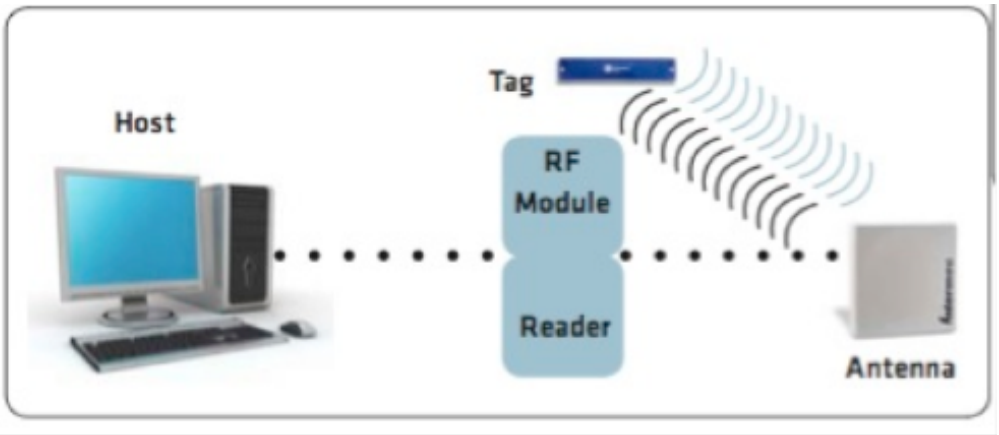

Figure 4: Working of a RFID System

RFIDs offer several advantages over typical data collection methods. Some of these are:

- RFIDs can be employed in hazardous conditions and used to monitor hazardous objects, in our case, containers with radioactive materials without any human intervention
- Since each tag is different, over a thousand reads can be performed in a single second with high accuracy and precision
- RFIDs provide stealth since its components: tags, readers, and antennas operate on radio frequency and can be hidden from plain sight. As a result, the system acts as a major theft deterrent

There are generally three types of RFID tags:

- Active RFID tags, which contain a battery, and transmit signals autonomously
- Passive RFID tags, which have no battery and require an external source to provoke signal transmission
- Battery Assisted Passive (BAP) RFID tags, which require an external source to wake up but have significant higher forward link capability providing greater range

Due to security considerations, an active (reader)-passive (tag) system is used in the safeguards system lab. An active – passive RFID system offers the advantage of continuous 24 hours monitoring. This is due to the fact that *passive* tags don't use any batteries and an *active* reader is always ON as it is connected to a steady power supply.

For simplicity, an Intermec IF4 in Figure 5 is employed as our choice of RFID reader. The IF4 works on an ultra high frequency (UHF) of 866 MHz - 868 MHz. The range and reader is chosen since it is the industry standard for supply chain management, asset tracking and interference avoidance. It uses RS232 and Programmable Logic Containers (PLCs) for a cost-effective implementation. The combination of RS232 and PLCs reduces communication load on the network since this protocol filters out unneeded data caused by multiple reads and reduces redundancy. It also solves one of the main challenges involving RFIDs – see section 2.4.

Figure 5: Intermec IF4 RFID System

3.1.3 Radiation Monitors

A radiation monitor (also known as a particle detector) is a device used to detect, track and/or identify high-energy particles, such as those produced by nuclear decay, cosmic radiation, or reactions in a particle accelerator. A summary of radiation monitors is outlined in the Chart 1[5].

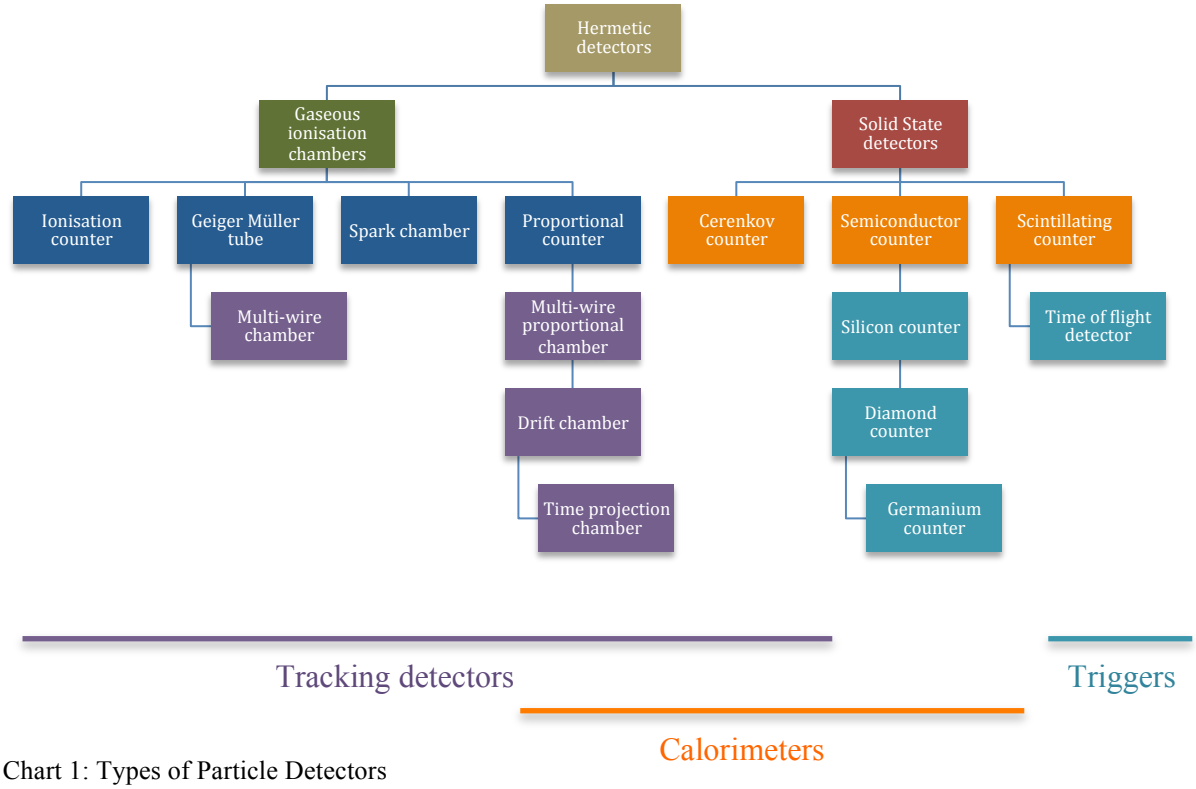

Chart 1: Types of Particle Detectors

Different types of radiation – sunlight, radio, and microwaves – surround us. Consisting mostly of electromagnetic waves, these are not dangerous due to low intensity or photon energy. Nuclear radiation, on the other hand, consists of:

- Particles (alpha, beta, and neutrons) and short-wavelength waves (gamma)
- High enough energy to ionize molecules and cause biological damage

The biological damage caused by nuclear radiation depends on the dose received. This in turn depends on the source intensity and the extent to which the source is shielded. All radiation sources follow the inverse-square law for intensity: the dose received is four times less than double the distance from the source.

In our experiments, we are dealing with gamma rays and X-rays which are one of the most severe forms of particles emitted. While both alpha and beta particles cause damage only when inhaled, ingested, or injected; gamma rays and X-rays travel at the speed of light and penetrate most objects without any change in wavelength. They can also pass through air almost unaffected. Because it is not easily attenuated, gamma-radiation is also the most common means of both detection of, and human exposure to, radiation sources [6]. Due to this and the fact that we need to monitor a limited area, Canberra G64 Area Gamma Monitor, shown in Figure 6, is the equipment of choice.

Figure 6: Canberra G64 Radiation Monitor

The G64, which has been designed specifically for monitoring areas in nuclear facilities, is a compact, mains-powered and mobile microprocessor based radiation monitor. The monitor enables us to display the gamma dose rate in the area and warn local personnel if the dose reaches above a preset limit by sounding an audible alarm. It allows for use in low to medium dose rate applications such as laboratory experiments and classroom teaching. Apart from these, it also offers the following advantages:

- Response time of less than 6 seconds for up to 90% change in the final step value
- Dynamic range, which allows for dose detections rates of as low as 10 μSv/h to as high as 100 mSv/h (10 μR/hr to 10 R/hr)

- Ion chamber detector option for use in high range application going from 100μSv/h to 100 Sv/h (10 mR/hr – 10 kR/hr)
- Remote detector unit for remote use that provides mobility to the system
- Allows for signaling the security personnel using visual and audio alarms

The G64 monitor operates on the principle of unit pulse. Gamma radiation incident on the G64 monitor produce pulses directly proportional to the incident energy and dose rate. The pulses are then converted to series of voltage pulses, which if higher than the preset level, trigger an alarm. At the same time, the data is sent out to the computer through RS232 cables to be displayed on the screen. Chart 2 shown below describes the flow of information pictorially [7].

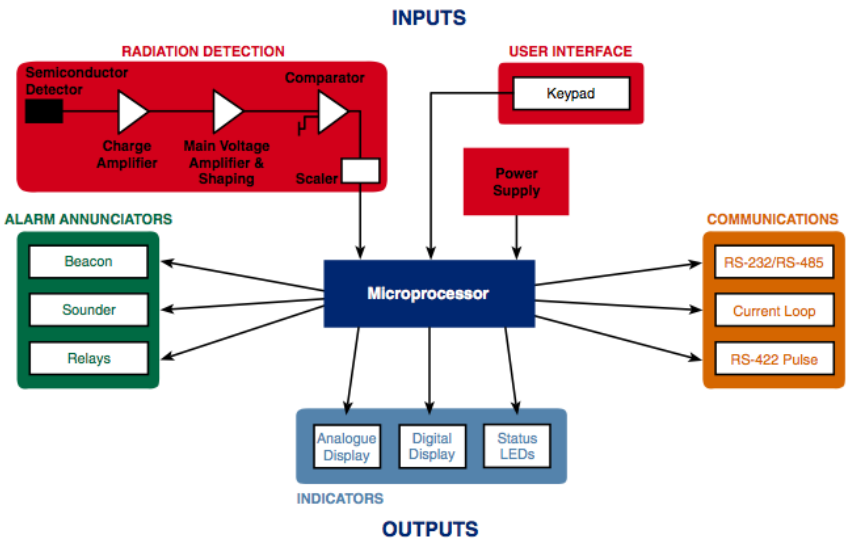

Chart 2: Working of Canberra G64 Radiation Monitor

3.2 Software

Building a system by combining the most expensive hardware available in the market does not equate to an efficient or a good system. In today's world, where hardware and software go hand-in-hand, it is imperative that well-written software drives the hardware. It is also essential that the software directs the hardware behavior and keeps the user informed through timely reports displaying relevant information. If anyone were to buy the most expensive computer available in the market but not have a good operating system to drive it, the computer is nothing except a big black box with flashing lights. As such, the main aim of this project is to develop an application that is not only smart and efficient, but can also integrate relevant information from a wide range of hardware irrespective of hardware manufacturer and display the information on a single screen. At the same time, the application should also be capable of driving automated processes to inform the user of critical events through an email or a message or archive the date for future access. We have developed separate applications for the three types of equipment used in the system. These are:

- An application to stream content from the camera system
    - Motion Detection Software
- An application to display information from the RFID system
- An application to show data from the Radiation Monitors

The content from the three above applications will be displayed in a single window through the use of tabs in an integrated application. The main purpose of this integrated application is to show all the information through a single medium rather than

having to switch between different applications each time a user wants to see any of the three components.

3.2.1 Camera Software

The benefits of using fixed IP and PTZ cameras are not limited to having good hardware but also extend to software. These cameras offer a variety of choices not only in terms of manufacturers but also in the number of image formats they support. Due to this, we developed an application which not only supports different camera manufacturers but also the various image formats. Some of the image formats supported by this application are:

- Joint Photographic Experts Group (JPEG)
- Motion Pictures Expert Group (MPEG)
- Microsoft Media Services (MMS)

Apart from the above formats, the application is entirely capable of supporting manufactures that include but are not limited to Axis, Panasonic, Star Dot, D-Link, and local devices such as a webcam or any other USB camera. In order to better understand the software development process, it is necessary to first get familiar with the workings of an IP camera. These cameras, as the name suggest can be plugged directly to an Ethernet switch and can be accessed over a network. They come equipped with a small-embedded computer whose purpose is to:

- Convert the binary data to a compressed digital image
- Display the image over the internet as per the request received

Since the final image is broadcast to an Internet address, IP cameras allow point access and remote access over any application that can access the Internet. These provide users with the flexibility of having access to the data anywhere in the world and allow use of the cameras in multiple scenarios. Figure 7 below provides an overview of the working of IP camera software [8].

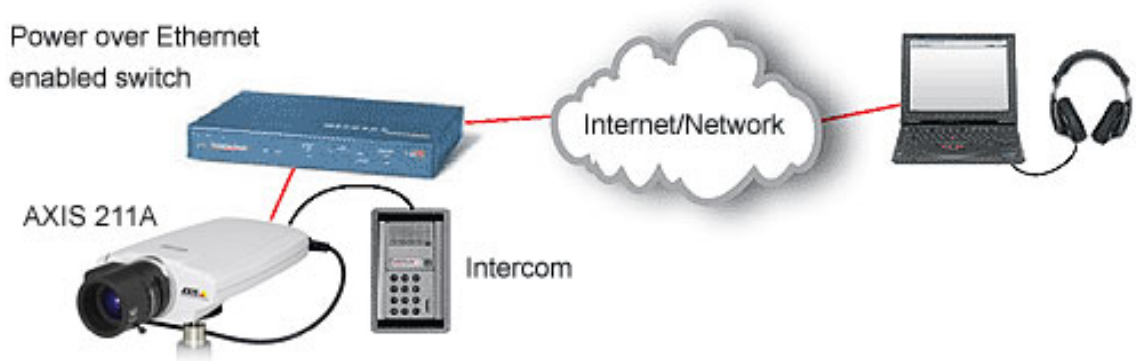

Figure 7: Overview of IP Camera Software

The simplest and most common image format broadcast by IP cameras is JPEG, which requires sending a request to the camera each time the user wants to view anything on the camera. Even though it allows the user to control the image refresh rate, this method is highly inefficient since each image refresh requires a new request that can only be sent once every few seconds. As a result, accessing and broadcasting JPEG

images can result in loss of valuable information since new images are displayed only after a certain number of seconds.

Due to this inefficiency, we use the cameras to access and broadcast MPEG and other video formats. The main advantage of this is that the program or the user needs to send a request only once for the camera to display images continuously. A predefined frame rate is sent with the request to make sure that we always see refreshed and new images on the screen. Below is a quick flow of the algorithm:

1. Send a HTTP request to the camera with a particular frame rate
2. Read the stream till the you reach the end of first frame and store it in a buffer
3. Read from the beginning to the end of next frame
4. Extract the binary data from the buffer, process it and display the image
5. Loop through steps 2 – 4

The main aim of the video application is to make sure it is flexible on the fly. It should be able to detect and start streaming images from the camera independent of its manufacturer.

Since video streaming is the most common feature across all cameras, an interface called *VideoStream* was created to satisfy this. After this, a group of classes was designed to contain the interface. Each class encapsulates all the communication data from the video interface and also extracts the image. All of these classes, however, are separate assemblies. And the user, to extend the functionality of the application, can add more classes. The *VideoStream* interface also contains abstract video provider

information classes. The addition of this abstract information class is necessary so that the application can handle different camera models from different manufacturers.

These abstract classes are then inherited by other interfaces such as *CamManufacturer* and *CamProperty*. The *CamManufacturer* interface contains precise information about the manufacturer such as different models and their configuration. The *CamProperty* interface is relevant since it loads up the video configuration properties for the particular model of the camera that is being used. Bringing together the three interfaces: *VideoStream, CamManufacturer* and *CamProperty*, creates a module for one manufacturer. Similarly, different modules can be created to include several different manufacturers.

When the application is executed, it finds all the relevant modules and collects information about the manufacturers that are present. After going through each and every file, it recalls the files implementing *VideoStream* and its dependencies. This search procedure is called only when the application is started. However, this can be changed to call the search whenever the user requests. For example, whenever the user adds a new manufacturer and wants to display the video feed without restarting the application, this is possible. All the user has to do is change the search procedure by clicking a few buttons.

3.2.1.2 Motion Detection Algorithm

The main purpose of developing and using a motion detection algorithm is to make the cameras more effective and automate the system response to a perceived

threat. This is particularly useful during the night time when security is usually at its lowest and threat levels are at their highest. It also helps us in overcoming storage constraints by saving only the events associated with “certain activity of interest” rather than recording everything cameras see the entire time.

Motion detection, as we all know, has become an integral part of any security system using cameras. Systems ranging from amateur home security projects to professional security installations at various sites all use motion detection in one form or another. The main goal here is to effectively capture any changes in the background, including but not limited to rippling water, shadows, and moving objects. A very popular technique is to model each pixel in a video frame with a distribution [9]. This method does not work very well in the case of dynamic natural environments such as the outdoors [10]. To deal with the limitation of such a parametric model, a non - parametric approach has been proposed. This approach uses the density estimation technique for building a statistical scene background [11]. These methods, however, do not consider the relationship between two neighboring pixels [12]. These conventional methods compare the current video frame to the previous or next video frame. This method is useful only when you need to write changes, not the whole frame and is not an ideal solution.

The developed algorithm is not based on any of the conventional approaches that are used today. It, however, takes a middle approach. In the developed algorithm:

1. A Background of the scene is created and is called *InitialFrame*.

2. Each frame, *NextFrame,* is compared to the background frame or the *InitialFrame*.
3. After this, the *InitialFrame* is incremented in the direction of the *NextFrame* at certain frame rate. The lower the frame rate, the more accurate is the comparison.
4. After this, a *Pixel* and *Adapt* filter is applied. The *Pixel* filter measures the change in pixel intensity as the frames progress and marks the area of change with a certain color.
5. The *Adapt* filter works on the basis of a percentage value specified by the user. If the user specifies a value of 50%, it will preserve 50% of the pixels in the *InitialFrame* image and 50% of the pixels in the *NextFrame* image. This allows the user to have control over the sensitivity of the motion detector algorithm. A 90% value will cause immediate updates in the *InitialFrame* image leading to constant refresh and very high sensitivity. After this, the changes are stored in a *temporary* image.
6. The *temporary* image is then merged with the background image to portray the change.
7. Steps 1 – 6 are repeated in a loop until the Motion Detector Algorithm is on.

The Motion Detector Algorithm can be triggered and disabled using code. It can also perform actions such as launching an application or sending an email. These options are completely configurable by the user and are extendable depending on the needs of the user.

3.2.2 RFID Middleware Algorithm

RFID is a means of wireless communication to identify a person or an object. A silicon chip connected to an antenna, often called a tag, communicates with a reader and sends in an identifier unique to the subject. The reader is a part of a network and is connected to an application on the host computer, which displays the information read from the tag. The communication frequencies used depend on the application, and range from 125 KHz to 2.45 GHz. Regulations are imposed by most countries (grouped into 3 regions) to control emission and prevent interference with other Industrial, Scientific and Medical equipment (ISM) [13]. The Intermec IF4 reader, for our application, operates on a frequency range of 865 – 868 MHz. A particular frequency is used in order to minimize the noise and disturbance from surroundings. However, this method does not remove the disturbance and is a subject of further research and technological advancement.

In our specific system, the software design required a new approach because of the sensitive material we are dealing with, limited hardware resources, and safety of the personnel. The most important factor to be considered is faultless reading of the ID tag. Because of this, the software itself has to detect all errors, find, and match the ID number of the tag or inform the user if a match is not found. Chart 3 provides an overview of the RFID software [14]:

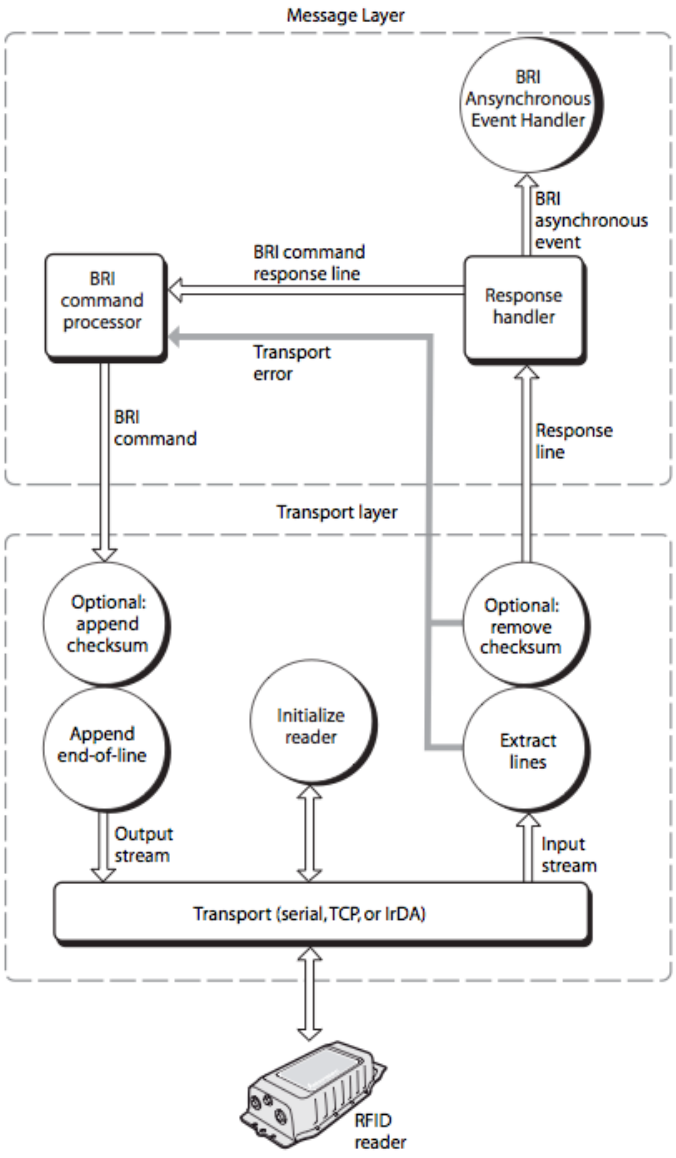

Chart 3: Overview of RFID Software

The algorithm for RFID software works in the following way:

1. The antenna broadcasts the optimal frequency stored in the microprocessor. For enhanced security and to prevent RFID tag spoofing, the user can change this value at any desired time.
2. The tags are activated after matching the frequency and send information (ID number) to the microcomputer. The information sent is an 8 - bit data code, no parity bit and one stop bit. The purpose of the stop bit is so that the reader separates the data from different tags if they are scanned in succession. This helps prevent unreliable or missed readings.
3. The tags are simultaneously compared to an internal database stored on the computer where the ID numbers are matched. For each matched ID, the tag count is incremented by 1 in a hash table. After this increment, the tag is disabled to prevent duplicate or multiple reads from the tag. This is done to avoid the stealing of radioactive containers and to prevent data redundancy, which was one of the problems, envisioned during the beginning of the project.
4. The tags then pass through a second antenna where the count is incremented by 1 again and stored in a hash table. The two hash table values are then compared and if found to be equal, the tag is marked as ‘exited’ and reset to 0 in the hash table.
5. The process is repeated in a loop for steps 1 – 4 for each tag.

Using this iterative algorithm and reading from two antennas solves two issues. First, we can keep a check on whether a tagged item is entering or exiting the area depending on the antenna it is scanned by first. Second, if the tag is read by one antenna and not by the second antenna in a matter of few seconds, the system raises a flag for the said antenna and reports it to the user as missing. This also gives the user an idea of the area in which to look for the missing container.

The RFID reader software is also capable of operating in two modes: SINGLESHOT and CONTINOUS mode [14]. These work in the following way:

- In SINGLESHOT mode, the reader executes the set number of IDTRIES or ANTTRIES, or continues reading until the timer expires, and returns all tags that are found. The number of tags found depends on the number of tags in the field. The SINGLESHOT mode may return NOTAG if no tags are present in the reader's field and the NOTAGRPT attribute is enabled. This mode is particularly useful if the user desires to run a quick check every interval to confirm the inventory count.
- In CONTINOUS mode, the reader continuously collects tags and stores the tags in an internal tag list. If the tag list gets full, the oldest tag in the list is removed. The usefulness of this mode is that it allows the user to automate the process of scanning the tags. The user can set the mode to CONTINOUS and let the system scan the tags on its own without enabling or disabling the reader for successive scans.

3.2.3 Radiation Monitor Algorithm

An overview of the radiation software is shown in Chart 4 [15]:

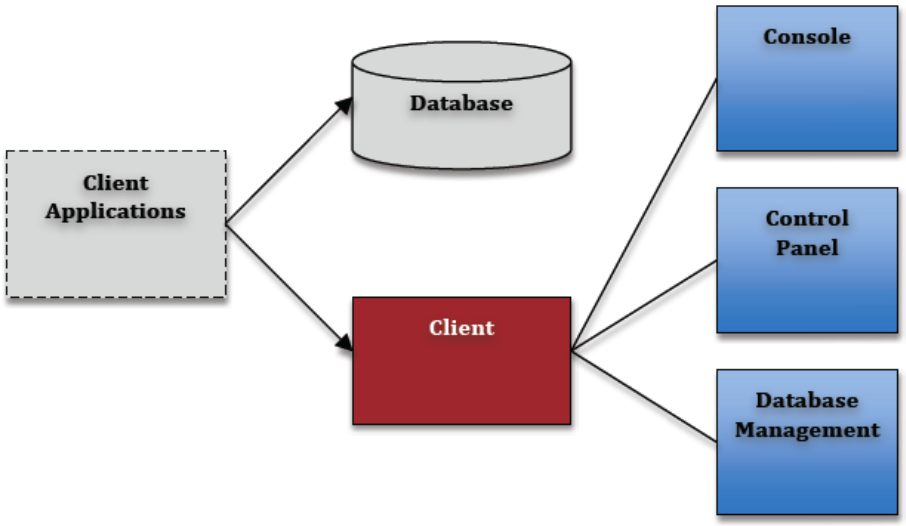

Chart 4: Overview of Radiation Detection Software

The G64 monitor operates on the principle of unit pulse. Gamma radiation incident on the G64 monitor produce pulses directly proportional to the incident energy and dose rate. These charge pulses are then amplified using the following factor:

$$factor = 1$$

They are then shaped to produce a series of voltage pulses, each of which, if above a certain threshold (set by the user) triggers an alarm. In order to compute the

radiation dose and display it on the screen, the following mathematical formulae and conversion factors are applied in the algorithm. First, a factor, *factor_G64*, recommended for converting the impulses to voltage for Canberra G-64 gamma monitor is applied:

$$factor\_G64 = \frac{1000.00}{1050.00}$$

Following this, to calculate the radiation dose per hour, *TotalDose* in μR/hr, we employ:

$$TotalDose(\mu R/hr) = factor\_G64 * counts/\min ute$$

The total time in seconds taken is computed using:

$$t(\sec) = \frac{d1}{dt} - \frac{d0}{dt}$$

After this, the total *current*, which is dependent on the impulse count over a specific time period, is calculated using:

$$current = (\frac{d1}{count} - \frac{d0}{count}) * TotalDose * \frac{60.0}{t}$$

After this, all the current values are stored in an array and compared to the maximum value that has been defined by the user. If any of the current values is greater than the maximum value defined, the alarm is triggered. If not, an average of all the current values is computed. If the average value is found to be higher than the maximum value an alarm is triggered.

The problem concerning area sweep of the radiation monitors is solved with the help of the 'Monte-Carlo' algorithm. The purpose is to model the area with Monte-Carlo

code to optimize the location of the radiation monitor for maximum radiation detection and will be used here for the same purpose.

3.2.4 Application Integration

While three separate applications achieve the purpose of providing an efficient MC&A system, it is still not very user friendly or desirable to monitor three separate applications. In order to unify the different applications, a tabbed interface is used. Tabbing is well known to most users today due to the widespread use of tabbed browsers. The solution thus offers a familiar interface to unify the various software components described in previous sections.

An application is uniquely identified through a process ID. Every application runs as an individual process and every running process has a unique process ID. An application is opened using the OpenProcess() function at which time a process ID is assigned to it. The integrated application uses these IDs to identify a list of running applications. The applications are presented to the user in a simple picker UI. The end-user simply has to pick the applications he/she wishes to see tabbed.

Once the MC&A systems component applications are selected, a new host window is created and the selected application windows are passed to it. Each of the selected applications now occupies a separate tab. Each tab retains the complete functionality and application specific menus. The applications that monitor visual surveillance, motion detection, RFID, and radiation detection together form the overall

MC&A system. These applications are now integrated into a single tabbed application that makes the system both simple and unified.

4. COST EFFECTIVENESS

One of the major goals of this research and development project is to design a system that is cost effective i.e. cheaper. In other words, the technology being developed should be able to deliver results and good service at a lower cost than current market practice. In order to understand the cost effectiveness of the developed system, it is necessary to know the difference between sites and facilities in the field of nuclear engineering and sciences.

A site is defined as a piece of land on which something is located. For example, a complete nuclear power plant located on a piece of land is defined as a site. A facility is defined as a building on a site. For example, any building on the nuclear power plant site is a facility on that particular site. As a result, a site contains more than one facility and each facility can have its own safeguards system.

If we look at the safeguards system from one of the top manufacturers in the nation, Canberra, it costs approximately $35,000. This cost is however only for the hardware components in the system and usually include cameras, containment systems (RFID), and radiation detection monitors. As with any system, it is essential to have the correct software for properly relaying data to the user for analysis. The cost of the software, which is separate from the hardware, can run more than $5,000. The cost breakup of such a commercial system from Canberra is listed in Table 1 below.

Table 1: Total Cost of a Commercially Available Safeguards System from Canberra

Components	Quantity	Unit Price
Environmental Radiation Monitoring Network	1	$35,000.00
IP Camera Software License	1	$999.00
RADACS System (Radiological Assessment Display and Control System)	1	$1,699.00
Total Cost Per System		37,698.00

As visible from the table above, the cost of installing such a system in one facility on a site can be $37,698.00. We know that a site has more than one facility and if we need to monitor each and every facility on the site, the total cost safeguards system can run into several $100,000 depending on the size of the site and number of facilities on a site.

On looking at the system that is being developed as a part of this research for a single facility (NSSPI) at the site (Texas A&M University), we see that it costs much lower compared to the commercial systems. Our system has the same hardware components (cameras, RFID, radiation monitors) as any other system available on the market. The breakdown of the cost system being developed is shown in Table 2 below.

Table 2: Total Cost of the Safeguards System Developed at NSSPI

Components	Quantity	Total Price
G64 Radiation Monitor	4	$20,000.00
Cameras	4	$2,080.00
RFID	2	$2,500
Total Cost Per System		$24,580.00

As can be seen from the two tables above, the cost per system being developed at NSSPI, Department of Nuclear Engineering at Texas A&M University, is over $13,000 less than the current commercially available system. If this system were being installed at each and every facility on a nuclear site, the overall savings will obviously be a very significant amount when compared to the market offerings. It is also possible that since this is the cost of a developing system, the final solution could cost far lesser when produced in bulk.

5. TESTING

Software testing has always been seen as a critical element of quality assurance. In order to ensure that the data is displayed properly and that all hardware components are communicating properly with the computer, testing needs to be thorough. A good test is one that has a high probability of finding a yet undiscovered error, and a successful test is one that uncovers a yet undiscovered error [16]. In our research, various testing methodologies were used. Testing was involved in each stage of the software life cycle, but testing done at each level of software development was different in nature and had different objectives. Software development and testing was done using Visual Studio 2005 and the Microsoft .NET Framework (Version 1.1, 2.0) was used to ensure compatibility with the Windows XP operating system. The model shown in Figure 8 was followed for testing:

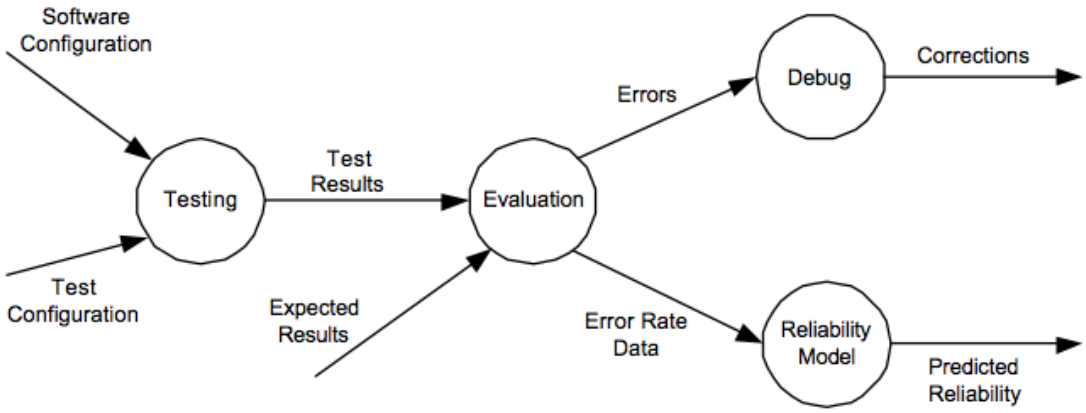

Figure 8: Software Testing Model

Unit testing was done at the lowest level. This involved testing a basic unit of software, which is the smallest piece or module that can be tested [16]. In the case of software for cameras, the simplest process involved making sure that the application framework which includes menus, maximize, minimize buttons and integration into the operating system had been executed properly. The next step involved creating and executing modules for different camera manufacturers and different image formats. These modules were then integrated into the application framework. After this the application was built, rebuilt and launched up to 20 times with other windows applications running in the background to ensure compatibility. The reruns showed several instances where the camera application stopped responding. On further research, this error was attributed to a bug in .Net Framework 1.0 and was fixed after the installation of .NET Framework 1.1 Service Pack 1.

A similar framework problem was encountered while developing the algorithm for motion detection. Apart from this, the fact that motion can range from being extremely slow to extremely fast, the choice is given to the user to choose motion sensitivity. Doing this allows the software to be adaptive to the needs of the user and less prone to errors since it is just calculating the difference between the pixel values in every frame. The results of both successful application builds are displayed in Figures 9 and 10.

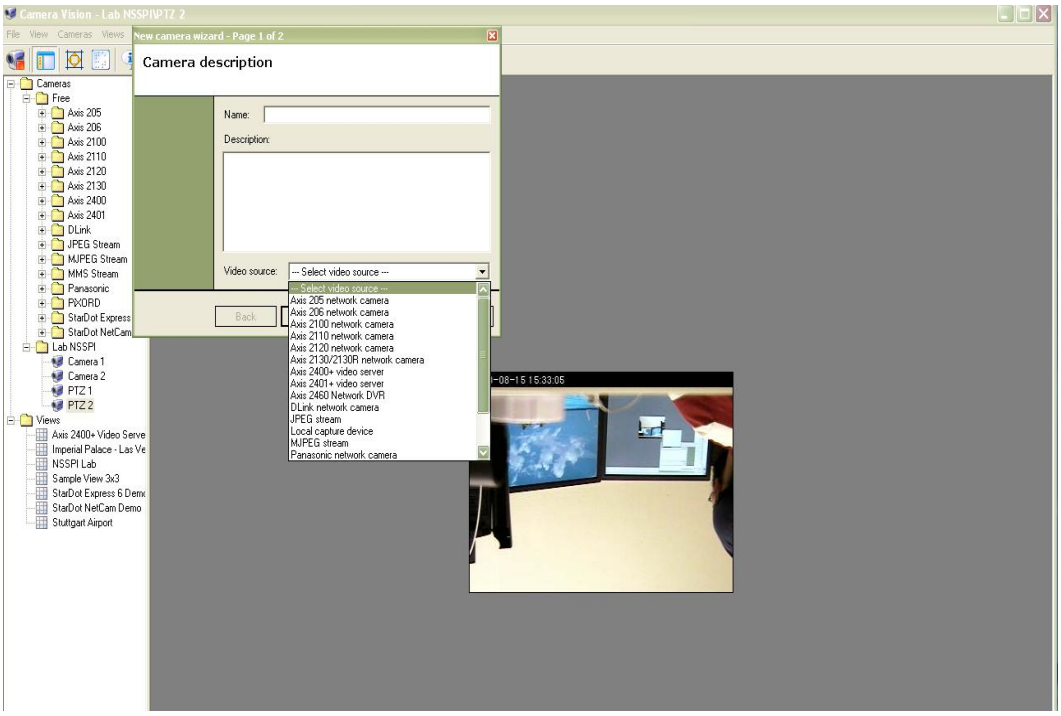

Figure 9: Results from Camera Software Testing

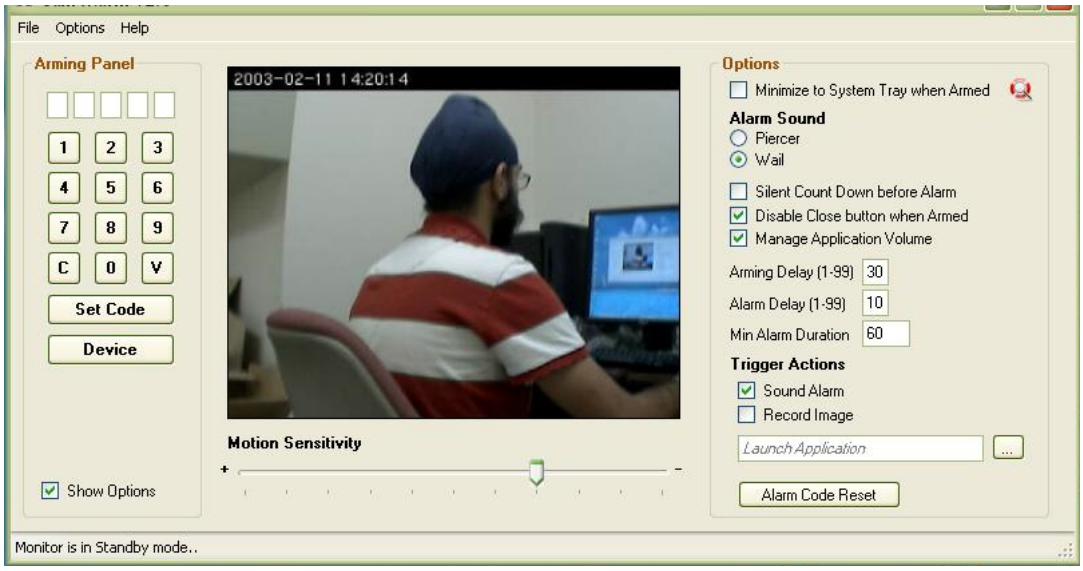

Figure 10: Results from Motion Detection Testing

Since the application framework was taken care of during the software development for the cameras, the main focus during the RFID middleware development was to ensure proper communication with the RS232 serial port. Being one of the most commonly used ports for communication and also the most erratic, the entire testing focused on communication and proper relaying of data from the RFID antenna to the software. Since the communication between the reader and computer is dependent on different software modules, each module was unit tested to ensure reliability. These modules were then integrated and 20 reruns of the RFID software were made to make sure the reader was online and communicated every time. A screenshot of the result is shown below in Figure 11.

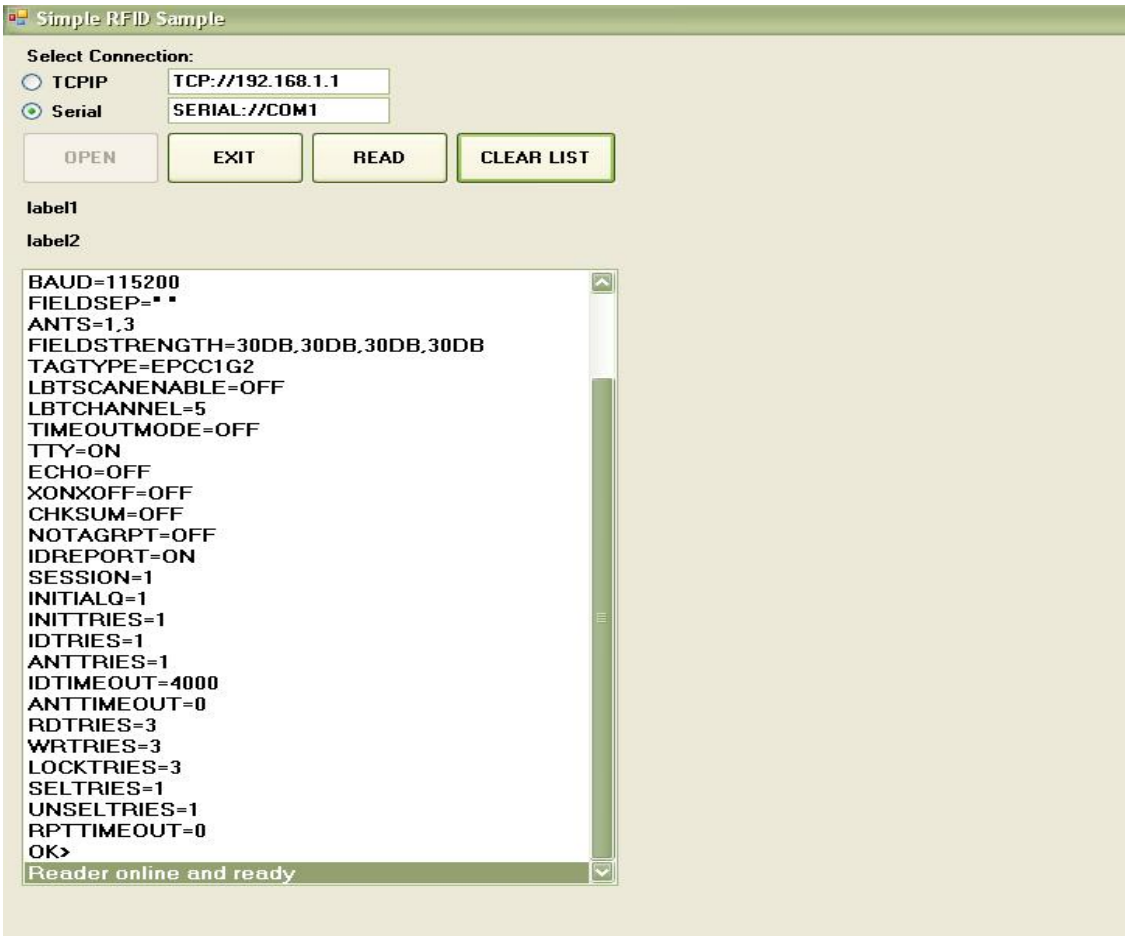

Figure 11: Results from RFID Software Testing

A protocol similar to RFID was followed for Radiation detection software. Since we are dealing with radiation dose rates that have a wide range, it was necessary to program the application so that it cover the maximum range possible. However, this

detected range is highly dependent on the hardware used and as a result, the user is given a choice to input the value to be detected to sound the alert, as shown in Figure 12.

Figure 12: Results from Radiation Software Testing

The last part involving integration proved to the hardest. Since there is no concrete way available to integrate different applications into one, we had to innovate here. The integrated application was tested using 1-5 applications at a time to ensure its compatibility with applications created on various frameworks. Testing with MDI containers proved to not work for applications that ran in child processes. Thus, the solution proposed was used. The integrated application was tested individually with the

motion detection, camera surveillance, RFID, and radiation detection software. The next phase involved testing various combinations of the above applications before testing the whole system together (multiple times).

6. RESULTS

The following series of images are screenshots of the software that has been developed for the safeguards system. The different software modules developed can run individually as well as an integrated piece of software. This gives the user capability to tweak and run the software as per the components used across different systems.

Figure 13 below shows the camera application. In the center, feed from the camera is displayed and the left side shows different models of cameras that can be recognized by the software.

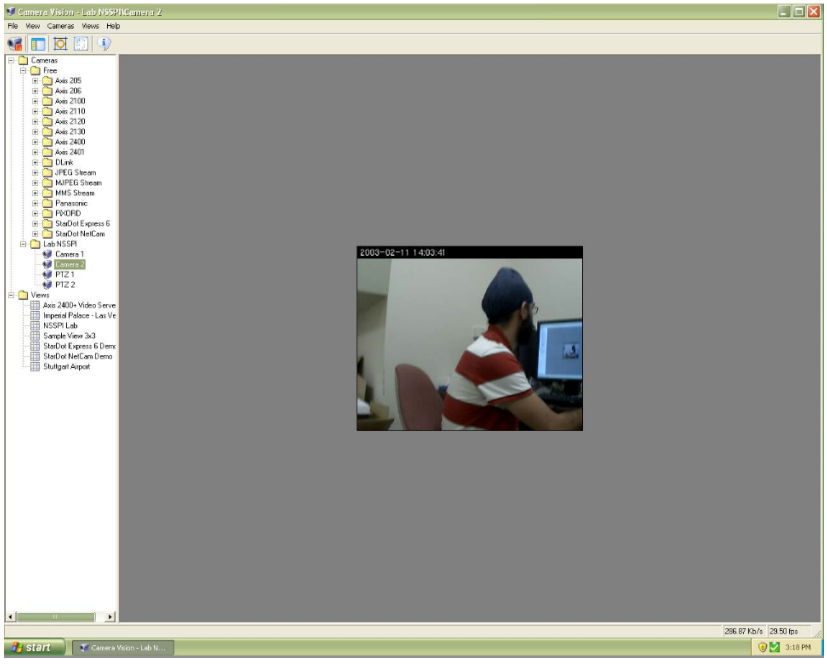

Figure 13: Results from the Camera Application Showing Feed from a Single Camera

Figure 14 demonstrates a 4x4 view, which shows output from all the cameras, used in the system. This view can also be modified to show up to 25 cameras.

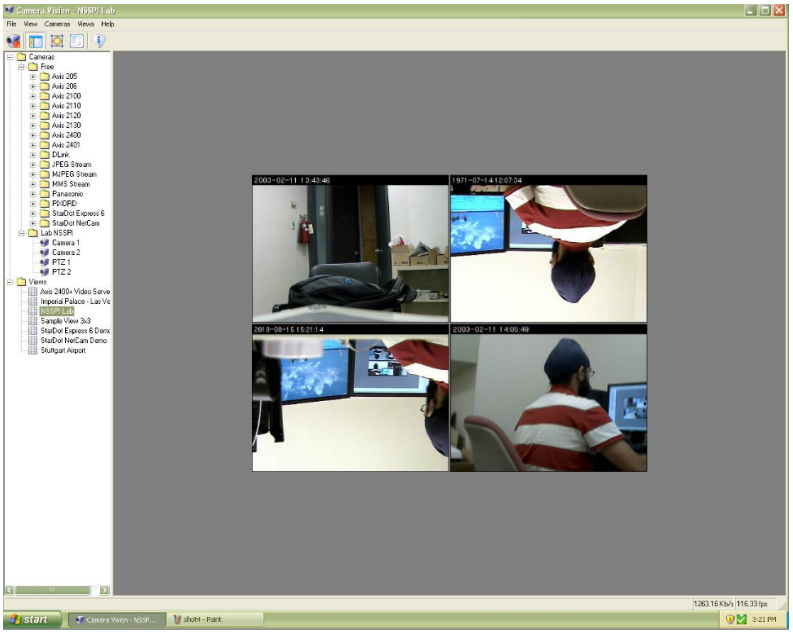

Figure 14: Results from the Camera Application Showing Feed from All Four Cameras

The application seen in the Figure 15 is the application that is used for displaying information read from RFID antennas. The application allows the user to attach up 4 RFID antennas using RS232 serial port. The application also has the capability to read from networked RFID antennas using TCP/IP protocol.

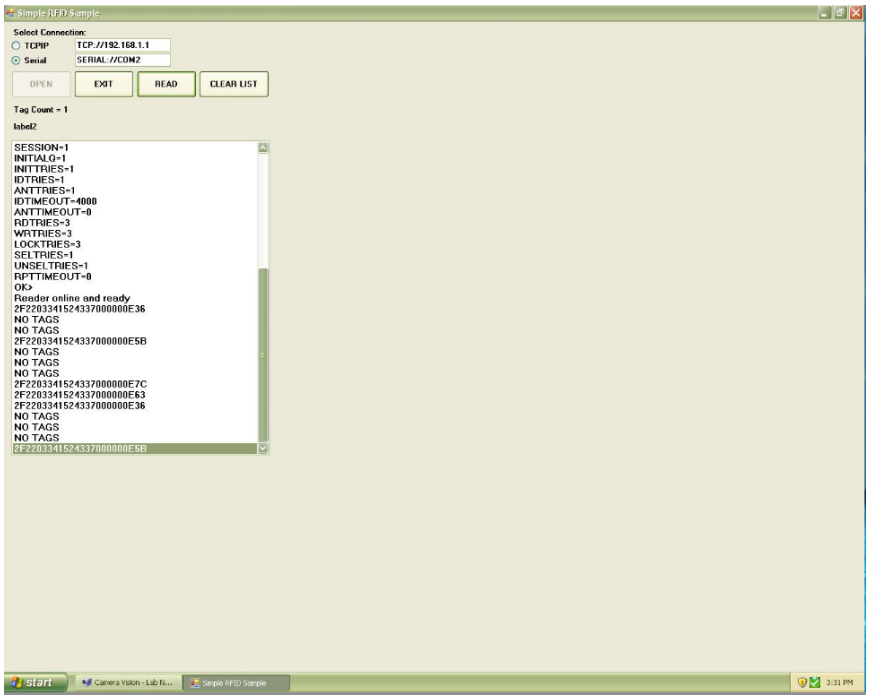

Figure 15: Results from the RFID App Showing Tag Readings

A screenshot from the motion detection application that has been developed alongside the camera application is displayed below in Figure 16. As visible from the screenshot, the application allows the user to enter a code to arm the alarm. It also allows the user to setup times before the alarm is sounded, the duration of the alarm time and adjust motion sensitivity. The areas where motion is detected are displayed in blue as can be seen. At the same time, the application is capable of various ‘Trigger Actions’ such as recording the image or launching certain applications when a motion is detected.

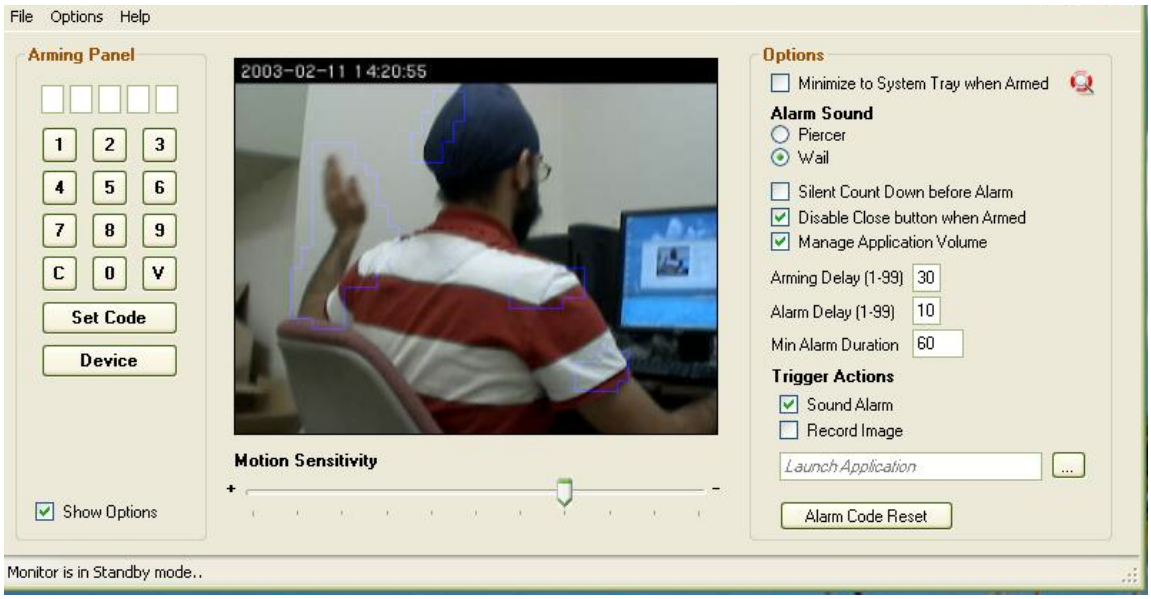

Figure 16: Results from the Motion Detection Application

The screenshot in Figure 17 is of the Digital Geiger Counter, which is the application for G64 Radiation Monitor. As seen, the application is capable of showing the counts per second on a time scale that ranges from seconds to a day. It also allows the user to set a peak value which when reached sets off an alarm. It is also capable of displaying various graphs such as line type, 3D line chart etc.

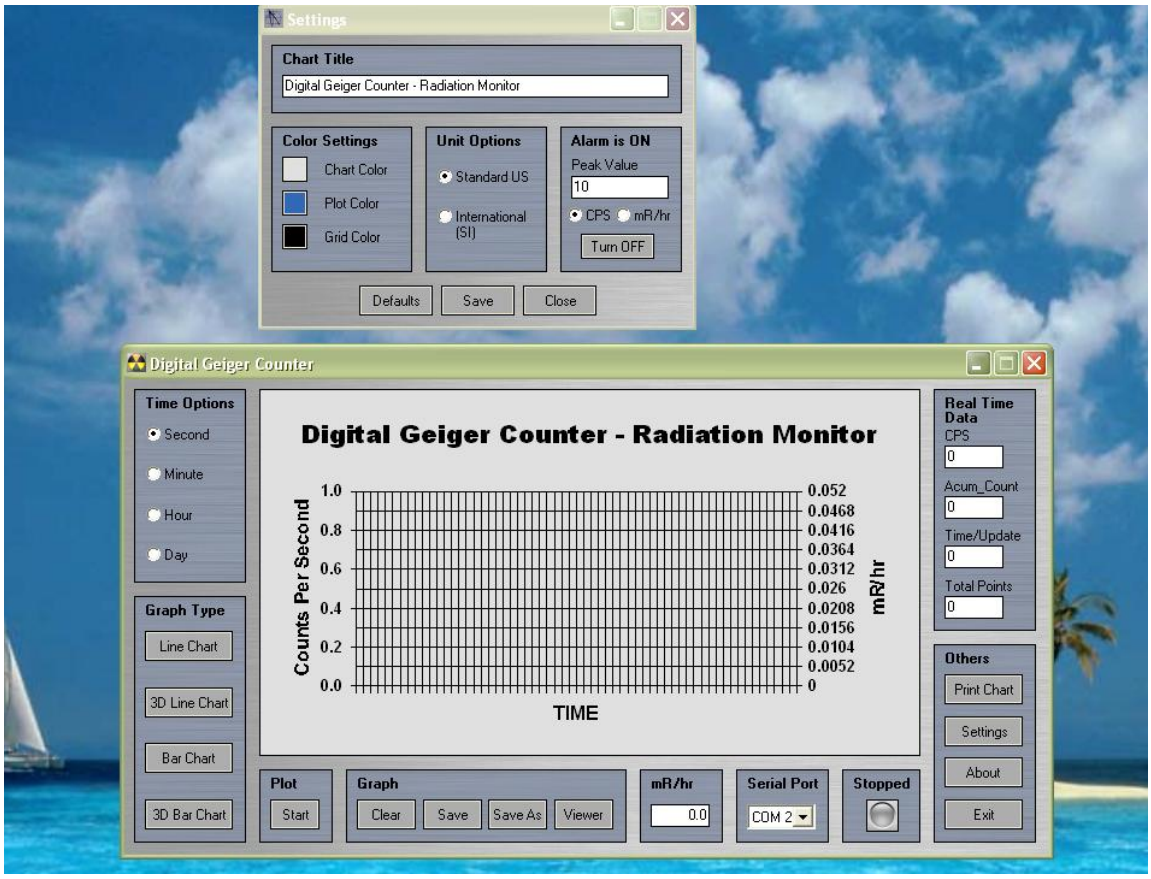

Figure 17: Results from the Radiation Detection Application

Figures 18, 19 and 20 are screenshots of the integrated application. As seen on the top of the window, all the above applications have been integrated into a single window with each application having a tab for itself in the integrated application. This allows the user to monitor the data from all the individual components in a single window without the need for maximizing, minimizing, or switching to different windows.

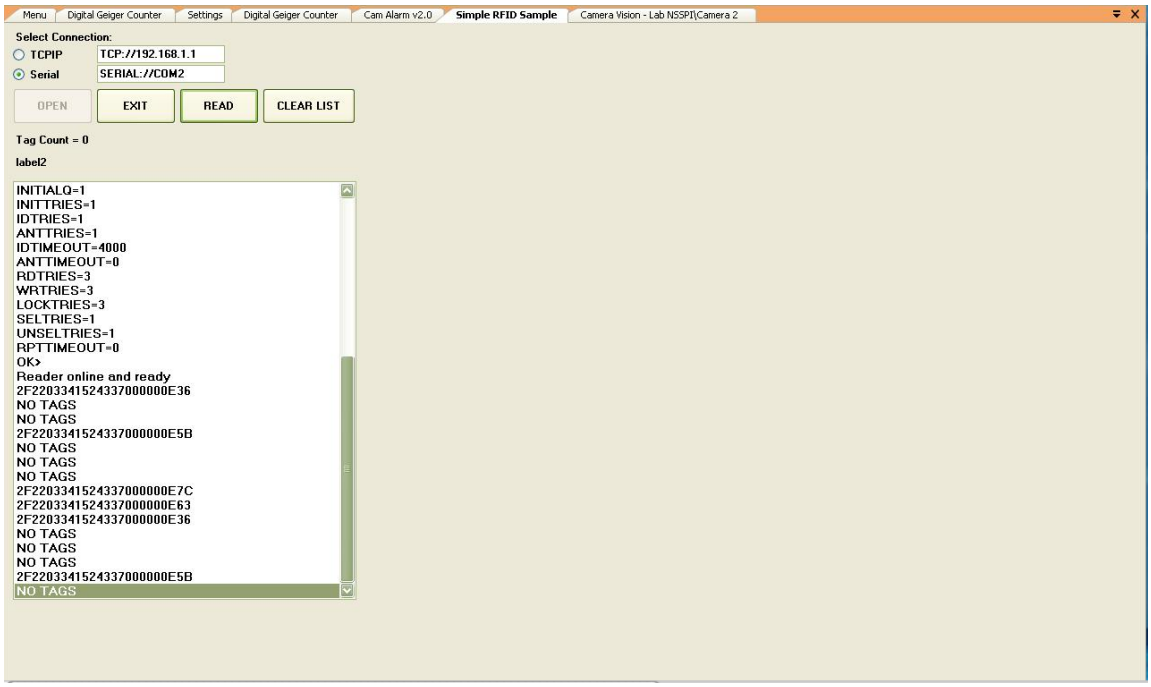

Figure 18: Integrated App Running All the Relevant System Applications. Currently Shows RFID App

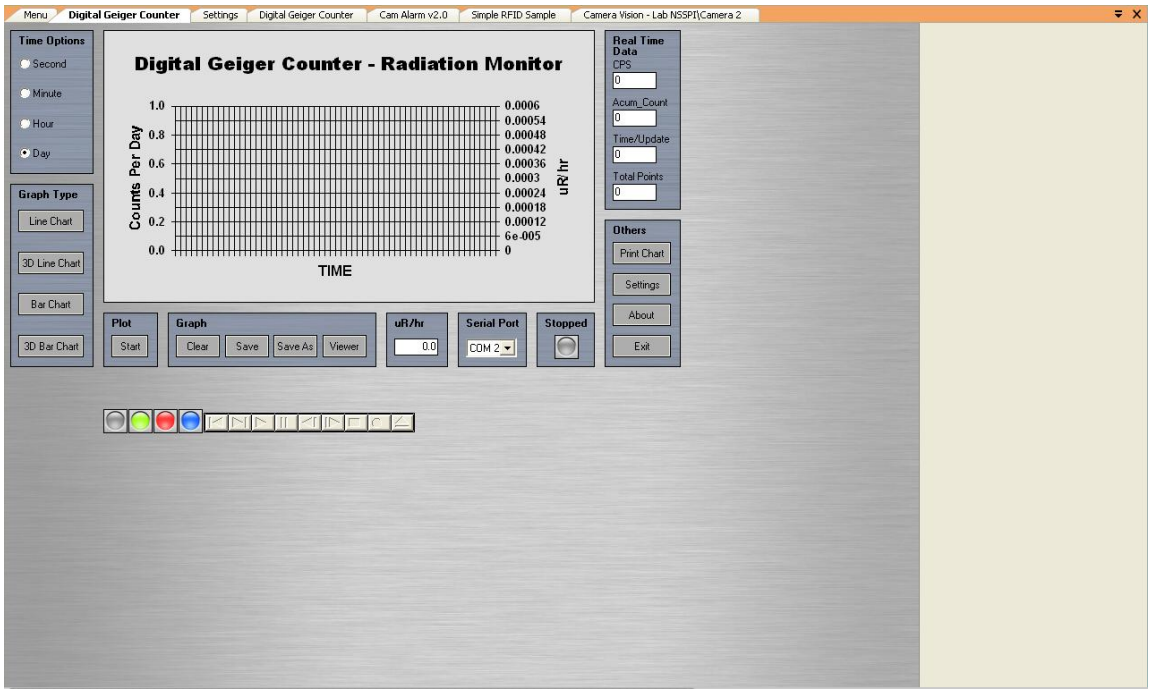

Figure 19: Integrated App Running All the Relevant System Applications. Currently Shows Radiation Detection App

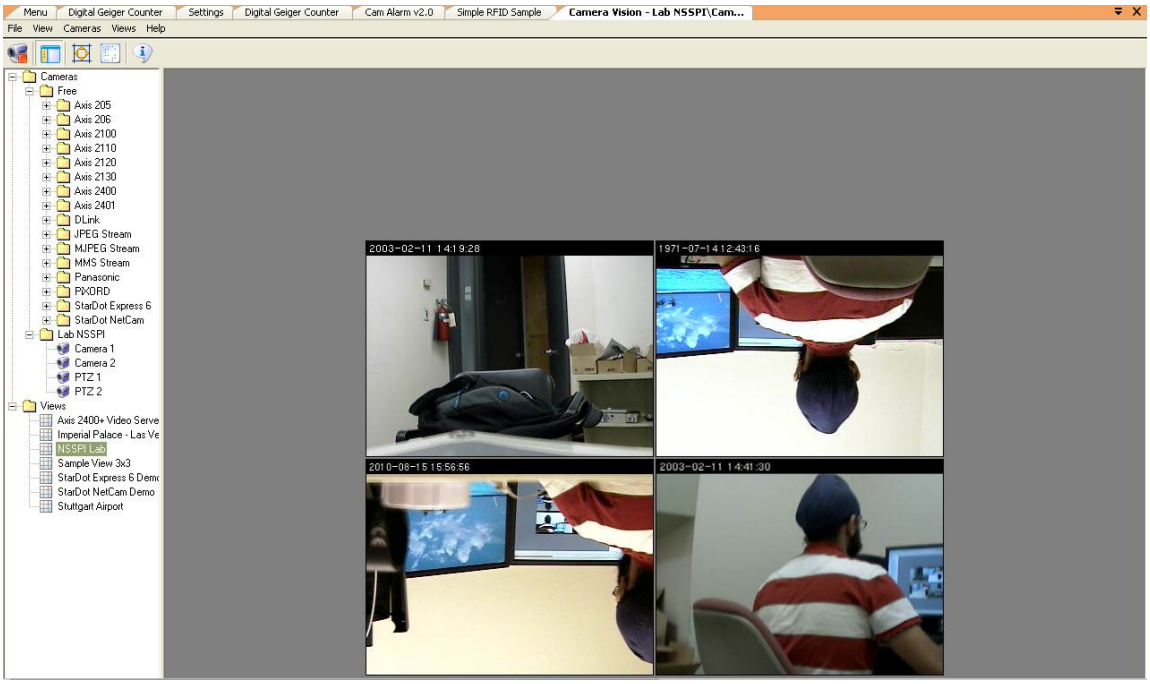

Figure 20: Integrated App Running All the Relevant System Applications. Currently Shows Camera App

7. CONCLUSION AND FUTURE WORK

The problems that emerge in the field of nuclear safeguard due to ever changing IAEA regulations has been solved in this thesis using a cost effective, integrated and smart approach. The solution to the problem consists of a new developed system that includes components such as Cameras, RFIDs, and Radiation Detection Monitors, which form the three pillars of an international safeguards system. Apart from this, the system that has been developed is customizable and can adapt to the needs of the user. It can also function well under different environments and over a wide range as shown in the results. In short, the solution proposed and developed solves all the present problems while being flexible, cost effective and reliable.

However, the developed system can be used for further research. Future research work in this area is outlined below:

1. First and foremost, it needs to be tested to make sure it can meet dynamic environments. This will include testing the system in different settings and facilities and making sure the responses from hardware are within certain established limits and meet all demands of the user.
2. Another potential area where future work can be performed is installation and beta testing of new equipment. For example, as research and development produce new and improved hardware such as cameras, RFID, and radiation monitors, it becomes important that these new technologies are tested before being incorporated in the field. One specific example of such type of equipment is Portal Monitors that are

usually installed at points of access such as border crossings, railroad tracks. Subjecting these monitors to thorough testing and different environments not only ensures what results can be expected but also highlights flaws in the equipment that may have been overlooked during limited testing by manufacturers.

3. Including advanced NDA equipment that has higher resolution and shorter count time will not only increase the reliability but also add to safety aspects of the system. This, however, will also increase the likelihood of false alarms as short counts of gamma rays from concrete can sound an alarm. On the other hand, if equipment with lower resolution and longer count time were used, safety and security may be compromised due to the inability of equipment to detect suspicious activity as proper time. As a result, further research needs to be done to incorporate NDA equipment having optimum resolution and count time.
4. Another area of future research that can further enhance the safeguards system is the inclusion of a biometric surveillance system. Addition of this technology to the present safeguards system will provide an extra blanket of security. However, the biometric technology is still in its infancy, hence, unreliable and expensive. The fact that biometrics deal with data that is very personal, further safeguards will be needed to ensure protection of such data.
5. Apart from the inclusions mentioned above, minimum detection thresholds need to be looked into for video cameras and motion detection. One major area of improvement related to these is resolution. Current security cameras have a maximum resolution of 640*480 pixels. Though sufficient for our current scenario, it

may not be enough to deal with threats in the future. It is a well-known observation that technologies that fool a security system are developed faster than a system can be upgraded. As a result, it is of prime importance that a minimum optimum threshold be established for graphic sensing to provide improved visual detection to the operator for the next few years. Another automated process that can improve visual surveillance is an algorithm that can automatically move the PTZ camera to the IP camera specified location when the motion detection algorithm sounds an alarm. One scenario where such an algorithm may fail is when both fixed IP and PTZ cameras are focused on different activities. This would require looking into images from all the cameras and letting the algorithm or user prioritize the activity. As such, both the prioritization and the automated algorithm can be further researched.

6. Similarly, optimum upper and lower radiation limits need to be established for further security and to detect small amounts to masking sources with background. Apart from the cameras and NDA equipment, limitations of RFID technology also exist and can compromise the system. As a result, work can be done to minimize interference and prevent spoofing of RFID frequency. One way this can be achieved is by changing the RFID frequency daily. Such a step, however, would require using multiple RFID readers and antennas. On the other hand, use of different radio frequencies may minimize spoofing but add to interference and cost of the system. A possible solution to this problem is to encrypt the radio waves with a security key. This, however, may not be easy in the current context and may also add to cost and

complexity of the system and needs to be further researched. Even though RFID has its advantages of allowing the tracking of an unlimited number of items, it is susceptible to spoofing and interference both of which can be minimized with further research.

7. Including the above optimizations in the system will definitely make the system more secure when compared to the options currently available. These system optimizations may take some time to develop and further more time to test. As a result, educational activities using laboratories are required. Such activities will not only subject the system to different scenarios and environments but will also reveal potential flaws that may have been overlooked during development.

In short, no safeguards system is truly and completely secure. Technologies that can fool a system are continually being developed along with the new system making development a continually evolving process. With an extra layer of research, testing and optimization, new and improved levels of security can easily be achieved.

REFERENCES

[1] J. E. Doyle, "Nuclear Security as a Multidisciplinary Field of Study," *Proceedings of the 8th International Conference on Facility Operations – Safeguards Interface*, 2008, pp 1-10.

[2] International Atomic Energy Agency, "Publications: IAEA Annual Report," *IAEA* [Online]. Available: http://www.iaea.org/Publications/Reports/index.html [Accessed: August 8, 2010].

[3] M. R. Rieback, G. N. Gaydadjiev, B. Crispo, R. F.H. Hofman, and A.S. Tenenbaum, "A Platform for RFID Security and Privacy Administration," *USENIX/SAGE Large Installation System Administration System Conference*, 2006, pp 1-14.

[4] A. Thomas, "ABCs of RFID: Understanding and Using Radio Frequency Identification," Everett, WA: Intermec Technologies Corporation, pp 1-6, 2007.

[5] H.M Stone Productions, Schloat, *Radiation Detectors*. Tarrytown, NY: Prentice-Hall Media, 1972.

[6] RAE Systems, "Basics of Nuclear Radiation," TN-176. San Jose, CA: RAE Systems, 2005.

[7] Canberra Industries, "G64 Area Gamma Monitor," C35772-G64-SS datasheet, Meridian, CO: Canberra Industries, 2007.

[8] Axis Communications, "AXIS 211A Network Camera – System overview | Axis Communications," *Axis Communications*. [Online].

Available: http://www.axis.com/products/cam_211a/overview.htm [Accessed: August 8, 2010].

[9] C. R. Wren, A. Azarbayejani, T. Darrell, and A.P. Pentland, "Pfinder: Real-Time Tracking of the Human Body," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp 780-785, 1997.

[10] B. Zhang, Y. Gao, T. Darrell, and B. Zhong, "Complex Background Modelling and Motion Detection Based on Texture Pattern Flow," *Proceedings of the 19th International Conference on Pattern Recognition*, 2008, pp 1-4.

[11] A. Elgammal, R. Duraiswami, D. Hardwood, and L.S. Davis, "Background and Foreground Modelling Using Nonparametric Kernel Density Estimation for Visual Surveillance," *Proceedings of the IEEE*, vol. 90, no. 7, pp 1151-1163, 2002.

[12] M. Heikkila, and M. Pietikainen, "A Texture-Based Method for Modelling the Background and Detecting Moving Objects," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 4, pp 657-662, 2006.

[13] M. Szczurkowsi, "Hardware and Software Solutions in RFID Reader System," *Proceedings of the 1st Conference*, 2006, pp 1-6.

[14] Intermec Technologies Technical Staff, "BRI Basic Reader Interface," Everett, WA: Intermec Technologies Corporation, pp 1-123, 2005.

[15] Canberra Industries, "Radiological Assessment Display and Control System," radacs datasheet, Meridian, CO: Canberra Industries, 2002.

[16] L. Luo, “Software Testing Techniques: Technology Maturation and Research Strategy,” Carnegie Mellon University, Pittsburgh, PA, Tech. Report 17-939A, 2006.

APPENDIX

Cameras

Accessing images from the cameras requires sending continuous request over HTTP to the cameras. Following this, the data is downloaded and images extracted from the downloaded data. A sample code of getting JPEG from the IP camera is:

```
string sourceURL = "http://webcam.mmhk.cz/axis-cgi/jpg/image.cgi";
byte[] buffer = new byte[100000];
int read, total = 0;

// create HTTP request
HttpWebRequest req = (HttpWebRequest) WebRequest.Create( sourceURL );

// get response
WebResponse resp = req.GetResponse( );

// get response stream
Stream stream = resp.GetResponseStream( );

// read data from stream
while ( ( read = stream.Read( buffer, total, 1000 ) ) != 0 )
{
   total += read;
}

// get bitmap
Bitmap bmp = (Bitmap) Bitmap.FromStream(
  new MemoryStream( buffer, 0, total ) );
```

In order to protect the camera with a password, the following command may be used:

```
// create HTTP request
```

```
HttpWebRequest req = (HttpWebRequest) WebRequest.Create( sourceURL );

// set login and password
req.Credentials = new NetworkCredential( login, password );
...
```

However, in order to extract MJPEG, the request needs to be sent only once.

Again, this is done using

```
--myboundary
Content-Type: image/jpeg

... image binary data ...

--myboundary
Content-Type: image/jpeg

... image binary data ...

--myboundary
Content-Type: image/jpeg

...
```

The URL format extract images from various cameras is as follows:

- Axis Cameras (for a full list, please refer to the Axis Cameras website)

  JPEG:
  http://<servername>/axis-cgi/jpg/image.cgi
  MJPEG:
  http://<servername>/axis-cgi/mjpg/video.cgi

- StarDot Cameras

  StarDot NetCam:
  http://<servername>/netcam.jpg

StarDot Express 6 (video server)
http://<servername>/jpeg.cgi?<cameranumber>
http://<servername>/jpeg.cgi?3

- PiXORD Cameras

  JPEG:
  http://<servername>/images<channel><resolution>
  http://<servername>/images1sif
  MJPEG:
  http://<servername>/getimage?camera=<channel>[&fmt=<re
  solution>][&delay=<delay>]
  http://<servername>/getimage?camera=1&fmt=sif&delay=10

- Panasonic Cameras

  JPEG:
  http://<servername>/SnapshotJPEG[?Resolution=<resolution>][&Quality=<qual
  ity>]
  http://<servername>/SnapshotJPEG?Resolution=320x240&Quality=Standard
  MJPEG:
  http://<servername>/nphMotionJpeg[?Resolution=<resolution>][&Quality=<qua
  lity>]
  http://<servername>/nphMotionJpeg?Resolution=320x240&Quality=Standard

- D-Link Cameras

  http://<servername>/cgi-bin/video.jpg

Motion Detection Algorithm

The motion detection algorithm being used is an iterative algorithm, which starts by choosing an initial frame as a background, and compares all the other frames to the background frame. The background frame changes every fixed number of intervals depending on the frames rate of the cameras. For example, if the camera being used has

a rate of 25 frames per second, the initial frame will change after every 25th frame. At the same time, percentage change in pixel density is calculated. This percentage change is flexible and can be adjusted by the user allowing him to control the sensitivity. The algorithm below describes how image is the initial frame is changed:

```
// alloc memory for a backgound image and for current image
backgroundFrame = new byte[len];
currentFrame = new byte[len];
currentFrameDilatated = new byte[len];

// lock image
BitmapData imgData = image.LockBits(new Rectangle( 0, 0, width, height ),
                    ImageLockMode.ReadOnly, PixelFormat.Format24bppRgb );

 // create initial backgroung image
PreprocessInputImage( imgData, width, height, backgroundFrame );

// unlock the image
image.UnlockBits( imgData );

// just return for the first time
return;
// move background towards current frame

for ( int i = 0; i < len; i++ )
{
int t = currentFrame[i] - backgroundFrame[i];
if ( t > 0 )
backgroundFrame[i]++;
else if ( t < 0 )
backgroundFrame[i]--;
}
```

The process to calculate the percentage change is done by the following:

```
// difference and thresholding
pixelsChanged = 0;
for ( int i = 0; i < len; i++ )
{
```

```
                int t = currentFrame[i] - backgroundFrame[i];
                if ( t < 0 )
                t = -t;
                if ( t >= 15 )
                {
                    pixelsChanged++;
                    currentFrame[i] = (byte) 255;
                }
                else
                {
                    currentFrame[i] = (byte) 0;
                }
}
```

RFID Middleware

The RFID middleware first establishes connection between the reader and computer using a serial port or a TCP/IP protocol. The code to perform this task is as:

```
private bool OpenReaderConnection()
{
        //Establish connection with reader.
        //Choose network or serial connection.
        bool bStatus = false;
        string sMsg = null;
        string sConnection = null;

        //define connection
        //string sConnection = "SERIAL://COM1";
        //string sConnection = "TCP://192.168.1.1";
        if (radioButton1.Checked == true)
        {
           //serial
           sConnection = textBox1.Text;
        }
        else
        {
           //tcpip
           sConnection = textBox2.Text;
        }
```

As mentioned previously, there are two modes for the RFID reader, SINGLESHOT and CONTINOUS mode. The SINGLESHOT mode is always enabled by default to aid in power saving. However, if one needs to change the mode to CONTINOUS, a parameter called REPORT needs to be used. This is done using the following commands:

> READ [DATA FIELD|LITERAL]*[TAGTYPE=<tagtype list>] [WHERE<data condition>] [PASSWORD=<"access_password">]
> [REPORT=EVENT|NO|EVENTALL] [STOP|POLL]

Setting REPORT = EVENT in the above command enables CONTINUOUS mode. The IDs are stored in a list and an event message is immediately reported for each tag, which is not on the list. REPORT = EVENTALL also does the same task as described in REPORT = EVENT. This setting, however, also returns the IDs that are continuously being read which does not happen in the former.

VITA

Name: Harneet Singh

Address: Department of Electrical and Computer Engineering,
Texas A&M University,
214 Zachry Engineering Center,
TAMU 3128
College Station, Texas 77843-3128

Email Address: harneet@neo.tamu.edu

Education: M.S., Electrical Engineering,
Texas A&M University, 2010

B.S., Electrical Engineering,
Texas A&M University, 2007